



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Seigo ARITA

Title: SECURE PARAMETER GENERATING DEVICE AND
PARAMETER GENERATING METHOD IN ALGEBRAIC CURVE
CRYPTOGRAPHY

Appl. No.: Unassigned

Filing Date: 8/25/2000

Examiner: Unassigned

Art Unit: Unassigned

*#2
Priority
Paper
MSA
10/20/00*

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

- Japan Patent Application No. 11-242075 filed 8/27/1999.

Respectfully submitted,

Date August 25, 2000

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

By *Phillip J. Artaola* Reg. No. 38,819
for/ David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

40405/325
Seigo ARITA

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JC864 U.S. PTO
09/645588
08/25/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年 8月27日

出 願 番 号
Application Number:

平成11年特許願第242075号

出 願 人
Applicant(s):

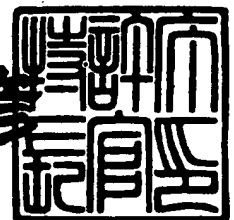
日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 6月 9日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3044421

【書類名】 特許願
 【整理番号】 33509589
 【あて先】 特許庁長官殿
 【国際特許分類】 G09C 1/00
 H04L 9/06

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日
 本電気株式会社内

【氏名】 有田 正剛

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100082935

【弁理士】

【氏名又は名称】 京本 直樹

【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100082924

【弁理士】

【氏名又は名称】 福田 修一

【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100085268

【弁理士】

【氏名又は名称】 河合 信明

【電話番号】 03-3454-1111

【手数料の表示】

【予納台帳番号】 008279

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9115699

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 代数曲線暗号における安全なパラメータの生成装置、生成方法、および記録媒体

【特許請求の範囲】

【請求項 1】

- (a) 曲線の複雑さの度合いを指定する2つの異なる素数 a 、 b 、および、使用したい暗号鍵のサイズ n を入力する入力装置と、
- (b) 前記入力手段に入力された素数 a 、素数 b 、暗号鍵のサイズ n をそれぞれ記憶する a 記憶手段、 b 記憶手段、および、 n 記憶手段と、
- (c) 前記 a 記憶手段、前記 b 記憶手段からそれぞれ素数 a 、素数 b を取得し、円の ab 分体におけるスティッケルバーガー要素 ω を演算するスティッケルバーガー要素計算装置と、
- (d) 前記スティッケルバーガー要素計算装置により演算されたスティッケルバーガー要素 ω を記憶する ω 記憶手段と、
- (e) 前記 a 記憶手段、前記 b 記憶手段、前記 n 記憶手段、前記 ω 記憶手段からそれぞれ素数 a 、素数 b 、暗号鍵のサイズ n 、スティッケルバーガー要素 ω を取得し、2つの異なる素数 a 、素数 b に対するヤコビ和候補値 j およびヤコビ和候補値 j に対応する素数 p を演算するヤコビ和候補値計算装置と、
- (f) 前記ヤコビ和候補値計算装置により演算された素数 p 、ヤコビ和候補値 j をそれぞれ記憶する p 記憶手段、および j 記憶手段と、
- (g) 前記 a 記憶手段、前記 b 記憶手段、前記 j 記憶手段から、それぞれ素数 a 、素数 b 、ヤコビ和候補値 j を取得し、素数 a 、素数 b で指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合 H を演算する位数候補値計算装置と、
- (h) 前記位数候補値計算装置により演算された集合 H を記憶する H 記憶手段と、
- (i) 前記 H 記憶手段から集合 H を取得し、集合 H の中から概素数性等の安全性条件を満たす候補値 h を検索する安全性判定装置と、
- (j) 前記安全性判定装置により検索された候補値 h を記憶する h 記憶手段と、
- (k) 前記 a 記憶手段、前記 b 記憶手段、前記 p 記憶手段、前記 h 記憶手段からそれぞれ素数 a 、素数 b 、素数 p 、候補値 h を取得し、素数 a 、素数 b 、素数 p で指定され

る代数曲線でそのヤコビアン群の位数が候補値 h と一致する代数曲線のパラメータを演算するパラメータ決定装置と、

前記パラメータ決定装置で演算された代数曲線のパラメータを出力する出力装置と、

を備えたことを特徴とする代数曲線暗号における安全なパラメータの生成装置。

【請求項 2】 前記 a 記憶手段、前記 b 記憶手段からそれぞれ素数 a 、素数 b を取得し、式 $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-1}^{-t}$ (t は ab を法とする既約剰余類の代表系を走り、 $[\lambda]$ は有理数 λ を超えない最大の整数を表し、 $\langle \lambda \rangle$ は有理数 λ の小数部分 $\lambda - [\lambda]$ を表し、 σ_t は円の ab 分体におけるガロア写像 $\zeta \rightarrow \zeta^t$ を表す(ζ は 1 の原始 ab 乗根))を用いてスティッケルバーガー要素 ω を演算する前記スティッケルバーガー要素計算装置を備えることを特徴とする請求項 1 記載の代数曲線暗号における安全なパラメータの生成装置。

【請求項 3】 前記 a 記憶手段、前記 b 記憶手段、前記 n 記憶手段、前記 ω 記憶手段からそれぞれ素数 a 、素数 b 、暗号鍵のサイズ n 、スティッケルバーガー要素 ω を取得し、 1 の原始 ab 乗根で生成される円分体 K の素イデアルを生成する代数的整数 γ で、その絶対ノルムが $2n/(a-1)(b-1)$ 程度のビット長の素数 p となる α をランダムに生成し、式 $j = \gamma^\omega$ を用いてヤコビ和候補値 j を演算する前記ヤコビ和候補値計算装置を備えることを特徴とする請求項 1 または 2 記載の代数曲線暗号における安全なパラメータの生成装置。

【請求項 4】 前記 a 記憶手段、前記 b 記憶手段、前記 j 記憶手段からそれぞれ素数 a 、素数 b 、ヤコビ和候補値 j を取得し、 1 以上 $2ab$ 以下の整数である各 k に対して、 ζ を 1 の原始 ab 乗根とするとき、式 $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ ($\text{Norm}_{K|Q}$ は、円の ab 分体 K におけるノルム写像)を用いて、パラメータ a 、 b で指定される代数曲線のヤコビアン群の位数の候補値 h_k を演算し、候補値の集合 $H = \{h_1, h_2, \dots, h_{2ab}\}$ を演算する前記位数候補値計算装置を備えることを特徴とする請求項 1、2、または 3 記載の代数曲線暗号における安全なパラメータの生成装置。

【請求項 5】 前記 a 記憶手段、前記 b 記憶手段、前記 p 記憶手段、前記 h 記憶手段からそれぞれ素数 a 、素数 b 、素数 p 、候補値 h を取得し、素数 p を法とする 1

の原始 a 乗根 ζ_a および1の原始 b 乗根 ζ_b を求め、1以上 a 以下の各整数 l 、および1以上 b 以下の各整数 m に対して、式 $\zeta_a^l y^a + \zeta_b^m x^b + 1 = 0$ で定義される代数曲線上のランダムな点 G を生成し、点 G の表すヤコビアン群における要素の h 倍を計算し、結果がヤコビアン群における単位元に等しいならば、素数 a 、素数 b で指定される代数曲線でそのヤコビアン群の位数が候補値 h と一致する代数曲線のパラメータとして p 、 ζ_a^l および ζ_b^m を出力する前記パラメータ決定装置を備えることを特徴とする請求項1、2、3または4記載の代数曲線暗号における安全なパラメータの生成装置。

【請求項6】

(a) a 記憶手段、 b 記憶手段からそれぞれ曲線の複雑さの度合いを指定する2つの異なる素数 a 、 b を取得し、円の ab 分体におけるスティッケルバーガー要素 ω を演算するスティッケルバーガー要素計算手順と、

(b) 前記スティッケルバーガー要素計算手順により演算されたスティッケルバーガー要素 ω を ω 記憶手段に記憶する手順と、

(c) 前記 a 記憶手段、前記 b 記憶手段、 n 記憶手段、前記 ω 記憶手段からそれぞれ素数 a 、素数 b 、暗号鍵のサイズ n 、スティッケルバーガー要素 ω を取得し、2つの異なる素数 a 、素数 b に対するヤコビ和候補値 j およびヤコビ和候補値 j に対応する素数 p を演算するヤコビ和候補値計算手順と、

(d) 前記ヤコビ和候補値計算手順により演算された素数 p 、ヤコビ和候補値 j をそれぞれ p 記憶手段、および j 記憶手段に記憶する手順と、

(e) 前記 a 記憶手段、前記 b 記憶手段、前記 j 記憶手段から、それぞれ素数 a 、素数 b 、ヤコビ和候補値 j を取得し、素数 a 、素数 b で指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合 H を演算する位数候補値計算手順と、

(f) 前記位数候補値計算手順により演算された集合 H を H 記憶手段に記憶する手順と、

(g) 前記 H 記憶手段から集合 H を取得し、集合 H の中から概素数性等の安全性条件を満たす候補値 h を検索する安全性判定手順と、

(h) 前記安全性判定手順により検索された候補値 h を h 記憶手段に記憶する手順と、

(i) 前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数a、素数b、素数pで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算するパラメータ決定手順と、
を含むことを特徴とする代数曲線暗号における安全なパラメータの生成方法。

【請求項7】 前記a記憶手段、前記b記憶手段からそれぞれ素数a、素数bを取得し、式 $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-1}^{-t}$ (tはabを法とする既約剰余類の代表系を走り、 $[\lambda]$ は有理数 λ を超えない最大の整数を表し、 $\langle \lambda \rangle$ は有理数 λ の小数部分 $\lambda - [\lambda]$ を表し、 σ_t は円のab分体におけるガロア写像 $\zeta \rightarrow \zeta^t$ を表す(ζ は1の原始ab乗根))を用いてスティッケルバーガー要素 ω を演算する前記スティッケルバーガー要素計算手順を含むことを特徴とする請求項6記載の代数曲線暗号における安全なパラメータの生成方法。

【請求項8】 前記a記憶手段、前記b記憶手段、前記n記憶手段、前記 ω 記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、スティッケルバーガー要素 ω を取得し、1の原始ab乗根で生成される円分体Kの素イデアルを生成する代数的整数 γ で、その絶対ノルムが $2n/(a-1)(b-1)$ 程度のビット長の素数pとなる α をランダムに生成し、式 $j = \gamma^\omega$ を用いてヤコビ和候補値jを演算する前記ヤコビ和候補値計算手順を含むことを特徴とする請求項6または7記載の代数曲線暗号における安全なパラメータの生成方法。

【請求項9】 前記a記憶手段、前記b記憶手段、前記j記憶手段からそれぞれ素数a、素数b、ヤコビ和候補値jを取得し、1以上2ab以下の整数である各kに対して、 ζ を1の原始ab乗根とすると、式 $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ ($\text{Norm}_{K|Q}$ は、円のab分体Kにおけるノルム写像)を用いて、パラメータa、bで指定される代数曲線のヤコビアン群の位数の候補値 h_k を演算し、候補値の集合 $H = \{h_1, h_2, \dots, h_{2ab}\}$ を演算する前記位数候補値計算手順を含むことを特徴とする請求項6、7、または8記載の代数曲線暗号における安全なパラメータの生成方法。

【請求項10】 前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数pを法とする

1 の原始 a 乗根 ζ_a および1 の原始 b 乗根 ζ_b を求め、1 以上 a 以下の各整数 l 、および1 以上 b 以下の各整数 m に対して、式 $\zeta_a^l Y^a + \zeta_b^m X^b + 1 = 0$ で定義される代数曲線上のランダムな点 G を生成し、点 G の表すヤコビアン群における要素の h 倍を計算し、結果がヤコビアン群における単位元に等しいならば、素数 a 、素数 b で指定される代数曲線でそのヤコビアン群の位数が候補値 h と一致する代数曲線のパラメータとして p 、 ζ_a^l および ζ_b^m を出力する前記パラメータ決定手順を含むことを特徴とする請求項 6、7、8 または 9 記載の代数曲線暗号における安全なパラメータの生成方法。

【請求項 1 1】

- (a) a 記憶手段、 b 記憶手段からそれぞれ曲線の複雑さの度合いを指定する2つの異なる素数 a 、 b を取得し、円の ab 分体におけるスティッケルバーガー要素 ω を演算するスティッケルバーガー要素計算手順と、
- (b) 前記スティッケルバーガー要素計算手順により演算されたスティッケルバーガー要素 ω を ω 記憶手段に記憶する手順と、
- (c) 前記 a 記憶手段、前記 b 記憶手段、 n 記憶手段、前記 ω 記憶手段からそれぞれ素数 a 、素数 b 、暗号鍵のサイズ n 、スティッケルバーガー要素 ω を取得し、2つの異なる素数 a 、素数 b に対するヤコビ和候補値 j およびヤコビ和候補値 j に対応する素数 p を演算するヤコビ和候補値計算手順と、
- (d) 前記ヤコビ和候補値計算手順により演算された素数 p 、ヤコビ和候補値 j をそれぞれ p 記憶手段、および j 記憶手段に記憶する手順と、
- (e) 前記 a 記憶手段、前記 b 記憶手段、前記 j 記憶手段から、それぞれ素数 a 、記憶手段 b 、ヤコビ和候補値 j を取得し、素数 a 、素数 b で指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合 H を演算する位数候補値計算手順と、
- (f) 前記位数候補値計算手順により演算された集合 H を H 記憶手段に記憶する手順と、
- (g) 前記 H 記憶手段から集合 H を取得し、集合 H の中から概素数性等の安全性条件を満たす候補値 h を検索する安全性判定手順と、
- (h) 前記安全性判定手順により検索された候補値 h を h 記憶手段に記憶する手順

と、

(i) 前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数a、素数b、素数pで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算するパラメータ決定手順と、

をコンピュータに実行させるプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、離散対数型暗号（以下、代数曲線暗号と記す）における安全なパラメータの生成装置、生成方法、および記録媒体に関し、特に、代数曲線のヤコビアン群を用いた離散対数型暗号における安全なパラメータの生成装置、生成方法、および記録媒体に関する。

【0002】

【従来の技術】

離散対数型暗号は、与えられた有限群上の離散対数問題の困難性に基づく公開鍵暗号方式である。暗号の安全性を保つためには、用いる有限群の位数は、ほぼ素数、すなわち、小さな整数と大きな素数の積でなければならない。離散対数型暗号の一種である代数曲線暗号では、ヤコビアン群の位数がほぼ素数である代数曲線を用いる必要がある。

【0003】

最も簡単な代数曲線である楕円曲線の場合には、任意の楕円曲線に対して、そのヤコビアン群の位数を計算する効率的なアルゴリズムが知られている。例えば、1995年、レネ＝スクーフ著、カウティング＝ポイントズ＝オン＝エリプティック＝カーブズ＝オーバー＝ファイナイト＝フィールズ、ジャーナル＝ドゥ＝セオリ＝ドゥ＝ノンブル、7巻、219-254 (Rene Schoof, Counting points on elliptic curves over finite fields, Journal de Theorie des Nombres, de Bordeaux x 7 (1995), 219-254, Institut de Mathematique de Bordeaux) に詳しい記述がある。ヤコビアン群の位数がほぼ素数である楕円曲線を得るには、上記のアルゴ

リズムを利用して、以下のようにすればよい。

【0004】

1. ランダムな楕円曲線Eを生成する。
2. Eのヤコビアン群の位数nを計算する。
3. nがほぼ素数ならばEを出力し、そうでないならば1に戻る。

【0005】

楕円曲線以外の代数曲線の場合には、例外的な一部の超楕円曲線を除いて、そのヤコビアン群の位数を計算する効率的なアルゴリズムは知られていない。そのため、代数曲線暗号で利用できる代数曲線は、楕円曲線および例外的な一部の超楕円曲線に限定されてしまう。

【0006】

また、ヤコビアン群における要素のh倍演算に関しては、「有田、吉川、宮内、 C_{ab} 曲線を用いた離散対数型暗号のソフトウェア実装、1999年暗号と情報セキュリティシンポジウム、pp.573-578」が知られている。

【0007】

また、「特開平6-282226号公報」記載の技術は、「任意の素数を選び、素数に対応した暗号化鍵を公開ファイル装置に登録し、素数、暗号鍵に対応する復号鍵表により生成し、素数と共に復号鍵表を復号装置に記憶しておき、暗号化装置が公開ファイル装置より受信者（復号装置）の公開鍵を入手し、平文を楕円曲線上で乗算し、その値を暗号文として復号装置に送信し、復号装置が暗号文から楕円曲線のパラメータを計算し、復号鍵表を用いてパラメータに対応する復号鍵を選び、暗号文を楕円曲線で乗算した値から中国剰余定理を用いて平文を得る」ものである。

【0008】

【発明が解決しようとする課題】

上述した従来技術においては、使用できる代数曲線が、楕円曲線および例外的な一部の超楕円曲線に限定されている。楕円曲線および超楕円曲線は、代数曲線全体から見ると、極めて特殊な代数曲線であり、暗号解読のためのターゲットが狭くなるため、代数曲線暗号の安全性に問題がある。

【0009】

本発明の目的は、従来使用できなかった高次の複雑な代数曲線を代数曲線暗号に用いることを可能とし、代数曲線暗号の安全性を向上させることである。

【0010】

【課題を解決するための手段】

本発明の第1の代数曲線暗号における安全なパラメータの生成装置は、

(a) 曲線の複雑さの度合いを指定する2つの異なる素数 a 、 b 、および、使用したい暗号鍵のサイズ n を入力する入力装置と、

(b) 前記入力手段に入力された素数 a 、素数 b 、暗号鍵のサイズ n をそれぞれ記憶する a 記憶手段、 b 記憶手段、および、 n 記憶手段と、

(c) 前記 a 記憶手段、前記 b 記憶手段からそれぞれ素数 a 、素数 b を取得し、円の ab 分体におけるスティッケルバーガー要素 ω を演算するスティッケルバーガー要素計算装置と、

(d) 前記スティッケルバーガー要素計算装置により演算されたスティッケルバーガー要素 ω を記憶する ω 記憶手段と、

(e) 前記 a 記憶手段、前記 b 記憶手段、前記 n 記憶手段、前記 ω 記憶手段からそれぞれ素数 a 、素数 b 、暗号鍵のサイズ n 、スティッケルバーガー要素 ω を取得し、2つの異なる素数 a 、素数 b に対するヤコビ和候補値 j およびヤコビ和候補値 j に対応する素数 p を演算するヤコビ和候補値計算装置と、

(f) 前記ヤコビ和候補値計算装置により演算された素数 p 、ヤコビ和候補値 j をそれぞれ記憶する p 記憶手段、および j 記憶手段と、

(g) 前記 a 記憶手段、前記 b 記憶手段、前記 j 記憶手段から、それぞれ素数 a 、素数 b 、ヤコビ和候補値 j を取得し、素数 a 、素数 b で指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合 H を演算する位数候補値計算装置と、

(h) 前記位数候補値計算装置により演算された集合 H を記憶する H 記憶手段と、

(i) 前記 H 記憶手段から集合 H を取得し、集合 H の中から概素数性等の安全性条件を満たす候補値 h を検索する安全性判定装置と、

(j) 前記安全性判定装置により検索された候補値 h を記憶する h 記憶手段と、

(k) 前記 a 記憶手段、前記 b 記憶手段、前記 p 記憶手段、前記 h 記憶手段からそれ

ぞれ素数 a 、素数 b 、素数 p 、候補値 h を取得し、素数 a 、素数 b 、素数 p で指定される代数曲線でそのヤコビアン群の位数が候補値 h と一致する代数曲線のパラメータを演算するパラメータ決定装置と、

前記パラメータ決定装置で演算された代数曲線のパラメータを出力する出力装置と、

を備える。

【0011】

本発明の第2の代数曲線暗号における安全なパラメータの生成装置は、前記第1の代数曲線暗号における安全なパラメータの生成装置であって、

前記 a 記憶手段、前記 b 記憶手段からそれぞれ素数 a 、素数 b を取得し、式 $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t^{-1}}$ (t は ab を法とする既約剰余類の代表系を走り、 $[\lambda]$ は有理数 λ を超えない最大の整数を表し、 $\langle \lambda \rangle$ は有理数 λ の小数部分 $\lambda - [\lambda]$ を表し、 σ_t は円の ab 分体におけるガロア写像 $\zeta \rightarrow \zeta^t$ を表す(ζ は1の原始 ab 乗根))を用いてスティッケルバーガー要素 ω を演算する前記スティッケルバーガー要素計算装置を備える。

【0012】

本発明の第3の代数曲線暗号における安全なパラメータの生成装置は、前記第1、または第2の代数曲線暗号における安全なパラメータの生成装置であって、前記 a 記憶手段、前記 b 記憶手段、前記 n 記憶手段、前記 ω 記憶手段からそれぞれ素数 a 、素数 b 、暗号鍵のサイズ n 、スティッケルバーガー要素 ω を取得し、1の原始 ab 乗根で生成される円分体 K の素イデアルを生成する代数的整数 γ で、その絶対ノルムが $2n/(a-1)(b-1)$ 程度のビット長の素数 p となる α をランダムに生成し、式 $j = \gamma^\omega$ を用いてヤコビ和候補値 j を演算する前記ヤコビ和候補値計算装置を備える。

【0013】

本発明の第4の代数曲線暗号における安全なパラメータの生成装置は、前記第1、第2、または第3の代数曲線暗号における安全なパラメータの生成装置であって、前記 a 記憶手段、前記 b 記憶手段、前記 j 記憶手段からそれぞれ素数 a 、素数 b 、ヤコビ和候補値 j を取得し、1以上 $2ab$ 以下の整数である各 k に対して、 ζ を1

の原始 ab 乗根とすると、式 $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ ($\text{Norm}_{K|Q}$ は、円の ab 分体 K におけるノルム写像) を用いて、パラメータ a 、 b で指定される代数曲線のヤコビアン群の位数の候補値 h_k を演算し、候補値の集合 $H = \{h_1, h_2, \dots, h_{2ab}\}$ を演算する前記位数候補値計算装置を備える。

【0014】

本発明の第5の代数曲線暗号における安全なパラメータの生成装置は、前記第1、第2、第3、または第4の代数曲線暗号における安全なパラメータの生成装置であって、前記 a 記憶手段、前記 b 記憶手段、前記 p 記憶手段、前記 h 記憶手段からそれぞれ素数 a 、素数 b 、素数 p 、候補値 h を取得し、素数 p を法とする1の原始 a 乗根 ζ_a および1の原始 b 乗根 ζ_b を求め、1以上 a 以下の各整数 l 、および1以上 b 以下の各整数 m に対して、式 $\zeta_a^l Y^a + \zeta_b^m X^b + 1 = 0$ で定義される代数曲線上のランダムな点 G を生成し、点 G の表すヤコビアン群における要素の h 倍を計算し、結果がヤコビアン群における単位元に等しいならば、素数 a 、素数 b で指定される代数曲線でそのヤコビアン群の位数が候補値 h と一致する代数曲線のパラメータとして p 、 ζ_a^l および ζ_b^m を出力する前記パラメータ決定装置を備える。

【0015】

本発明の第1の代数曲線暗号における安全なパラメータの生成方法は、

- (a) a 記憶手段、 b 記憶手段からそれぞれ曲線の複雑さの度合いを指定する2つの異なる素数 a 、 b を取得し、円の ab 分体におけるスティッケルバーガー要素 ω を演算するスティッケルバーガー要素計算手順と、
- (b) 前記スティッケルバーガー要素計算手順により演算されたスティッケルバーガー要素 ω を ω 記憶手段に記憶する手順と、
- (c) 前記 a 記憶手段、前記 b 記憶手段、 n 記憶手段、前記 ω 記憶手段からそれぞれ素数 a 、素数 b 、暗号鍵のサイズ n 、スティッケルバーガー要素 ω を取得し、2つの異なる素数 a 、素数 b に対するヤコビ和候補値 j およびヤコビ和候補値 j に対応する素数 p を演算するヤコビ和候補値計算手順と、
- (d) 前記ヤコビ和候補値計算手順により演算された素数 p 、ヤコビ和候補値 j をそれぞれ p 記憶手段、および j 記憶手段に記憶する手順と、
- (e) 前記 a 記憶手段、前記 b 記憶手段、前記 j 記憶手段から、それぞれ素数 a 、素

数 b 、ヤコビ和候補値 j を取得し、素数 a 、素数 b で指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合 H を演算する位数候補値計算手順と、

(f) 前記位数候補値計算手順により演算された集合 H を H 記憶手段に記憶する手順と、

(g) 前記 H 記憶手段から集合 H を取得し、集合 H の中から概素数性等の安全性条件を満たす候補値 h を検索する安全性判定手順と、

(h) 前記安全性判定手順により検索された候補値 h を h 記憶手段に記憶する手順と、

(i) 前記 a 記憶手段、前記 b 記憶手段、前記 p 記憶手段、前記 h 記憶手段からそれぞれ素数 a 、素数 b 、素数 p 、候補値 h を取得し、素数 a 、素数 b 、素数 p で指定される代数曲線でそのヤコビアン群の位数が候補値 h と一致する代数曲線のパラメータを演算するパラメータ決定手順と、
を含む。

【0016】

本発明の第2の代数曲線暗号における安全なパラメータの生成方法は、前記第1の代数曲線暗号における安全なパラメータの生成方法であって、前記 a 記憶手段、前記 b 記憶手段からそれぞれ素数 a 、素数 b を取得し、式 $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t^{-1}}$ (t は ab を法とする既約剰余類の代表系を走り、 $[\lambda]$ は有理数 λ を超えない最大の整数を表し、 $\langle \lambda \rangle$ は有理数 λ の小数部分 $\lambda - [\lambda]$ を表し、 σ_t は \mathbb{F}_{ab} におけるガロア写像 $\zeta \rightarrow \zeta^t$ を表す(ζ は1の原始 ab 乗根))を用いてスティッケルバーガー要素 ω を演算する前記スティッケルバーガー要素計算手順を含む。

【0017】

本発明の第3の代数曲線暗号における安全なパラメータの生成方法は、前記第1、または第2の代数曲線暗号における安全なパラメータの生成方法であって、前記 a 記憶手段、前記 b 記憶手段、前記 n 記憶手段、前記 ω 記憶手段からそれぞれ素数 a 、素数 b 、暗号鍵のサイズ n 、スティッケルバーガー要素 ω を取得し、1の原始 ab 乗根で生成される \mathbb{F}_{ab} 分体 K の素イデアルを生成する代数的整数 γ で、その絶対ノルムが $2n/(a-1)(b-1)$ 程度のビット長の素数 p となる α をランダムに生成し

、式 $j = \gamma^\omega$ を用いてヤコビ和候補値 j を演算する前記ヤコビ和候補値計算手順を含む。

【0018】

本発明の第4の代数曲線暗号における安全なパラメータの生成方法は、前記第1、第2、または第3の代数曲線暗号における安全なパラメータの生成方法であって、前記a記憶手段、前記b記憶手段、前記j記憶手段からそれぞれ素数a、素数b、ヤコビ和候補値 j を取得し、1以上 $2ab$ 以下の整数である各 k に対して、 ζ を1の原始 ab 乗根とすると、式 $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ ($\text{Norm}_{K|Q}$ は、 \mathbb{F}_q の ab 分体 K におけるノルム写像) を用いて、パラメータa、bで指定される代数曲線のヤコビアン群の位数の候補値 h_k を演算し、候補値の集合 $H = \{h_1, h_2, \dots, h_{2ab}\}$ を演算する前記位数候補値計算手順を含む。

【0019】

本発明の第5の代数曲線暗号における安全なパラメータの生成方法は、前記第1、第2、第3、または第4の代数曲線暗号における安全なパラメータの生成方法であって、前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値 h を取得し、素数pを法とする1の原始a乗根 ζ_a および1の原始b乗根 ζ_b を求め、1以上a以下の各整数 l 、および1以上b以下の各整数 m に対して、式 $\zeta_a^l Y^a + \zeta_b^m X^b + 1 = 0$ で定義される代数曲線上のランダムな点Gを生成し、点Gの表すヤコビアン群における要素の h 倍を計算し、結果がヤコビアン群における単位元に等しいならば、素数a、素数bで指定される代数曲線でそのヤコビアン群の位数が候補値 h と一致する代数曲線のパラメータとしてp、 ζ_a^l および ζ_b^m を出力する前記パラメータ決定手順を含む。

【0020】

本発明の記録媒体は、

(a) a記憶手段、b記憶手段からそれぞれ曲線の複雑さの度合いを指定する2つの異なる素数a、bを取得し、 \mathbb{F}_q の ab 分体におけるスティッケルバーガー要素 ω を演算するスティッケルバーガー要素計算手順と、

(b) 前記スティッケルバーガー要素計算手順により演算されたスティッケルバーガー要素 ω を ω 記憶手段に記憶する手順と、

(c) 前記a記憶手段、前記b記憶手段、n記憶手段、前記 ω 記憶手段からそれぞれ素数a、素数b、暗号鍵のサイズn、ステイッケルバーガー要素 ω を取得し、2つの異なる素数a、素数bに対するヤコビ和候補値jおよびヤコビ和候補値jに対応する素数pを演算するヤコビ和候補値計算手順と、

(d) 前記ヤコビ和候補値計算手順により演算された素数p、ヤコビ和候補値jをそれぞれp記憶手段、およびj記憶手段に記憶する手順と、

(e) 前記a記憶手段、前記b記憶手段、前記j記憶手段から、それぞれ素数a、記憶手段b、ヤコビ和候補値jを取得し、素数a、素数bで指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合Hを演算する位数候補値計算手順と、

(f) 前記位数候補値計算手順により演算された集合HをH記憶手段に記憶する手順と、

(g) 前記H記憶手段から集合Hを取得し、集合Hの中から概素数性等の安全性条件を満たす候補値hを検索する安全性判定手順と、

(h) 前記安全性判定手順により検索された候補値hをh記憶手段に記憶する手順と、

(i) 前記a記憶手段、前記b記憶手段、前記p記憶手段、前記h記憶手段からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数a、素数b、素数pで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算するパラメータ決定手順と、

をコンピュータに実行させるプログラムを記録する。

【0021】

【発明の実施の形態】

まず、本発明の原理について説明する。

【0022】

本発明は、 $\alpha Y^a + \beta X^b + 1 = 0$ という形の定義方程式をもつ代数曲線のクラスから、そのヤコビアン群の位数がほぼ素数である代数曲線を効率的に探索し、従来使用できなかった高次の複雑な代数曲線を代数曲線暗号に用いることを可能にするものである。ここで、パラメータa、bは曲線の複雑さの程度を表す。

【0 0 2 3】

$\alpha Y^a + \beta X^b + 1 = 0$ という形の定義方程式をもつ、位数 q の有限体 F_q 上の代数曲線を $C(q, \alpha, \beta)$ とおく。代数曲線 $C(q, \alpha, \beta)$ に対しては、その L 関数がヤコビ和を用いて記述されることを用いて、そのヤコビアン群の位数を設計することができるのである。以下簡単のため、 $q := p$ (p を q とおく) は素数であり、 $p \equiv 1 \pmod{\text{LCM}(a, b)}$ とする (LCM は最小公倍数)。また、 1 の原始 ab 乗根を ζ とおく。素数 p は円分体 $Q(\zeta)$ において、 m 個の素イデアル P_1, P_2, \dots, P_m に完全分解する。ここで、 m は、法 ab の既約剰余類の個数である。

【0 0 2 4】

有限体 F_p の乗法群 F_p^* の生成元 w を固定し、 $(p-1)s$ が整数となる有理数 s に対して、 F_p^* の指標 χ_s を $\chi_s(w) = \exp(2\pi i s)$ (i は虚数) によって定義する。 $\chi_s(0) = 0$ (s : 整数でないとき)、 $= 1$ (s : 整数のとき) として、定義域を F_p 全体に拡張する。整数 $l=1, 2, \dots, a-1$ および整数 $m=1, 2, \dots, b-1$ に対して、 $j_p(l, m) = \sum_{\{1+v_1+v_2=0\}} \chi_{l/a}(v_1) \chi_{m/b}(v_2)$ はヤコビ和と呼ばれる。ここで、 v_1, v_2 は $1+v_1+v_2=0$ を満たす $v_1, v_2 \in F_p$ を走る。このとき、 $C(p, \alpha, \beta)$ の L 関数 $L_p(U)$ は以下のようにヤコビ和を用いて表されることが知られている。

【0 0 2 5】

$$L_p(U) = \prod_{l=1, 2, \dots, a-1, m=1, 2, \dots, b-1} (1 + \chi_{l/a}(\alpha^{-1}) \chi_{m/b}(\beta^{-1}) j_p(l, m) U).$$

したがって、 $C(p, \alpha, \beta)$ のヤコビアン群の位数 h は、

$$h = L_p(1) = \prod_{l=1, 2, \dots, a-1, m=1, 2, \dots, b-1} (1 + \chi_{l/a}(\alpha^{-1}) \chi_{m/b}(\beta^{-1}) j_p(l, m))$$

で与えられる。よって、ヤコビアン群の位数を求めるには、ヤコビ和 $j_p(l, m)$ が計算できればよい。しかしながら、ヤコビ和 $j_p(l, m)$ を定義式に従って直接計算することは計算量的に不可能なので、次のヤコビ和に対するスティッケルバーガー要素を用いる。

【0 0 2 6】

$[\lambda]$ は有理数 λ を超えない最大の整数を表し、 $\langle \lambda \rangle$ は有理数 λ の小数部分 $\lambda - [\lambda]$ を表すとする。また、 σ_t は円分体 $Q(\zeta)$ のガロア写像 $\zeta \rightarrow \zeta^t$ を表すとする。

る。群環 $Z[Gal(Q(\xi)|Q)]$ の元であるスティッケルバーガー要素 $\omega(a, b)$ を、
 $\omega(a, b) = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t}^{-1}$ とおく。

ただし、 t は、 ab を法とする既約剰余類の代表系を走るとする。

【0 0 2 7】

このとき、円分体 $Q(\xi)$ のイデアルとして、 $(j_p(1, m)) = P^{\omega(a, b)}$ が成立することが知られている。ここで、 P は p の上にある素イデアルである。上式より、 $j_p(1, m)$ は 1 の $2ab$ 乗根を除いて一意に定まる。そのうち、 ab 乗根分の自由度は $C(p, \alpha, \beta)$ の係数 $\alpha, \beta \in F_q$ の自由度から得られる。

【0 0 2 8】

以上より、次のような安全な曲線 $C(p, \alpha, \beta)$ の探索アルゴリズムが得られる。

安全な曲線 $C(p, \alpha, \beta)$ の探索アルゴリズム

入力: ヤコビアン の ビット 数 n

出力: p, α, β

(1) $g \leftarrow (a-1)(b-1)/2$

(2) ある n/g ビット 程度 の 素数 p に対する ヤコビ和 の 候補 j を 後述 の ヤコビ和 の 候補値 の 計算アルゴリズム を 用いて 探す:

$(p, j) \leftarrow \{\text{ヤコビ和の候補値の計算アルゴリズム}\}(n/g)$ 。

(3) 各 $k = 0, 1, \dots, ab$ に対して、

$h_k \leftarrow \prod_{l=1, 2, \dots, a-1, m=1, 2, \dots, b-1} (1 + (-\xi)^k j)$

(4) $\{h_0, h_1, \dots, h_{ab}\}$ に ほぼ素数 である h_k があるかどうかを調べる。
 なければ、(1) へ 戻る。あれば、 $h := h_k$ とする。

(5) ξ_a, ξ_b をそれぞれ F_p における 1 の a 乗根、 b 乗根とする。各 $l = 0, 1, \dots, a-1$ および 各 $m = 0, 1, \dots, b-1$ に対して、曲線 $C(p, \xi_a^l, \xi_b^m)$: $\xi_a^l y^a + \xi_b^m x^b + 1 = 0$ の ヤコビアン群 の オーダー が h に 等しいかどうか 調べる。等しければ、 $p, \alpha = \xi_a^l, \beta = \xi_b^m$ を 出力して 終了する。そのような l, m がなければ、(2) へ。

上で用いた、ヤコビ和の候補値の計算アルゴリズムでは、前記のスティッケルバーガー要素 $\omega(a, b) = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t}^{-1}$ を用いて、ヤコビ和の候補

値を求める。

ヤコビ和の候補値の計算アルゴリズムは以下のである。

入力: ビット数 m 、

出力: p 、 j 、

(1) $\omega \leftarrow \sum_t (\langle t/a \rangle + \langle t/b \rangle) \sigma_{-t}^{-1}$ 、

(2) $\gamma_0 = \sum_{l=0}^{m-1} c_l \zeta^l$ ($-10 < c_l < 10$) をランダムに生成。

(3) 各 $i = 1, 2, \dots$ に対して、

$\gamma \leftarrow \gamma_0 + 1$ 、

$p \leftarrow \text{Norm}_Q(\zeta) | Q(\gamma)$ 、

p が約 m ビットより小さいか？、

yes \rightarrow continue、

p が約 m ビットより大きい？、

yes \rightarrow (2) へ、

p が素数か？

no \rightarrow continue、

(4) $j \leftarrow \gamma^\omega$ 、 p および j を出力して終了。

【0029】

次に、本発明の第1の実施の形態について図面を参照して詳細に説明する。

【0030】

図1は、本発明の第1の実施の形態を示すブロック図である。

図1を参照すると、本発明の第1の実施の形態は、スティッケルバーガー要素計算装置11と、ヤコビ和候補値計算装置12と、位数候補値計算装置13と、安全性判定装置14と、パラメータ決定装置15と、メモリ16と、入力装置17と、出力装置18と、中央処理装置19とから構成される。

【0031】

また、メモリ16は、a記憶ファイル161、b記憶ファイル162、 ω 記憶ファイル163、j記憶ファイル164、H記憶ファイル165、h記憶ファイル166、p記憶ファイル167、および、n記憶ファイル168を含む。

【0032】

以下では、円分体 $Q(\zeta)$ における代数的数の四則演算、およびノルム $N_{Q(\zeta)|Q}$ の演算、および円分体 $Q(\zeta)$ に対するガロア群 $G(Q(\zeta)|Q)$ の作用の演算、および整数環 Z 係数のガロア群 $G(Q(\zeta)|Q)$ 上の群環 $Z[G(Q(\zeta)|Q)]$ における加法および乗法演算に関しては、既知の手法を用いるものとする。

【0033】

次に、本発明の第1の実施の形態の動作について説明する。

図2は、スティッケルバーガー要素計算装置11の動作を示すフローチャートである。

図3は、ヤコビ和候補値計算装置12の動作を示すフローチャートである。

図4は、位数候補値計算装置13の動作を示すフローチャートである。

図5は、パラメータ決定装置15の動作を示すフローチャートである。

【0034】

曲線の複雑さの度合いを指定する2つの異なる素数 $a=3$ 、 $b=7$ 、および使用したい暗号鍵のサイズ $n=160$ が入力装置17から入力された場合について説明する。入力された a 、 b は中央処理装置19を介してそれぞれ a 記憶ファイル161、 b 記憶ファイル162に一時的に記憶される。また、以下の記述において現れる変数は、メモリ16に格納される。

【0035】

次に、スティッケルバーガー要素計算装置11が、図2に示す処理にしたがって、 a 記憶ファイル161、 b 記憶ファイル162より $a=3$ 、 $b=7$ を取得して以下のように動作する。

【0036】

図2のステップS21において、変数 L に $a \cdot b = 3 \times 7 = 21$ を法とする既約剰余類の代表系 $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ が格納される。

【0037】

次に、図2のステップS22において、変数 $L = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ に含まれる各整数 t に対して、例えば、 $t=1$ のとき、 $[\langle 1/3 \rangle + \langle 1/7 \rangle] = [1/3 + 1/7] = [10/21] = 0$ なので、変数 m に0が格納され、 $-1^{-1} \equiv -1 \equiv 20 \pmod{21}$ なので、変数 s に20が格納され、 $0 \times \sigma_{20} = 0$ なので、変数 λ_1 に0が格納され

る。

【0038】

他のtについても同様にして、変数 λ_2 に $[\langle 2/3 \rangle + \langle 2/7 \rangle] = [2/3 + 2/7] = [20/21] = 0$ なので0が、変数 λ_4 に $[\langle 4/3 \rangle + \langle 4/7 \rangle] = [1/3 + 4/7] = [19/21] = 0$ なので0が、変数 λ_5 に $[\langle 5/3 \rangle + \langle 5/7 \rangle] = [2/3 + 5/7] = [29/21] = 1$ で $(-5)^{-1} \equiv 16^{-1} \equiv 4 \pmod{21}$ なので σ_4 が、変数 λ_8 に $[\langle 8/3 \rangle + \langle 8/7 \rangle] = [2/3 + 1/7] = [17/21] = 0$ なので0が、変数 λ_{10} に $[\langle 10/3 \rangle + \langle 10/7 \rangle] = [1/3 + 3/7] = [16/21] = 0$ なので0が、変数 λ_{11} に $[\langle 11/3 \rangle + \langle 11/7 \rangle] = [2/3 + 4/7] = [26/21] = 1$ で $(-11)^{-1} \equiv 10^{-1} \equiv 19 \pmod{21}$ なので σ_{19} が、変数 λ_{13} に $[\langle 13/3 \rangle + \langle 13/7 \rangle] = [1/3 + 6/7] = [25/21] = 1$ で $(-13)^{-1} \equiv 8^{-1} \equiv 8 \pmod{21}$ なので σ_8 が、変数 λ_{16} に $[\langle 16/3 \rangle + \langle 16/7 \rangle] = [1/3 + 2/7] = [13/21] = 0$ なので0が、変数 λ_{17} に $[\langle 17/3 \rangle + \langle 17/7 \rangle] = [2/3 + 3/7] = [23/21] = 1$ で $(-17)^{-1} \equiv 4^{-1} \equiv 16 \pmod{21}$ なので σ_{16} が、変数 λ_{19} に $[\langle 19/3 \rangle + \langle 19/7 \rangle] = [1/3 + 5/7] = [22/21] = 1$ で $(-19)^{-1} \equiv 2^{-1} \equiv 11 \pmod{21}$ なので σ_{11} が、変数 λ_{20} に $[\langle 20/3 \rangle + \langle 20/7 \rangle] = [2/3 + 6/7] = [32/21] = 1$ で $(-20)^{-1} \equiv 1^{-1} \equiv 1 \pmod{21}$ なので σ_1 が、それぞれ格納される。

【0039】

次に、図2のステップS2.3において、各変数 λ_1 、 λ_2 、 λ_4 、 λ_5 、 λ_8 、 λ_{10} 、 λ_{11} 、 λ_{13} 、 λ_{16} 、 λ_{17} 、 λ_{19} 、 λ_{20} に記憶された全データの総和 $\omega = \sigma_4 + \sigma_{19} + \sigma_8 + \sigma_{16} + \sigma_{11} + \sigma_1$ が計算される。ここでの総和は、群環 $Z[G(Q(\xi)|Q)]$ における総和であり、各 σ_i をシンボルとみなし、各 σ_i ごとの係数の総和を意味する。演算結果である ω は中央処理装置19を介して、 ω 記憶ファイル163に一時的に記憶される。

【0040】

次に、ヤコビ和候補値計算装置12が、a記憶ファイル161、b記憶ファイル162、n記憶ファイル168、 ω 記憶ファイル163から、 $a=3$ 、 $b=7$ 、 $n=160$ 、 $\omega = \sigma_4 + \sigma_{19} + \sigma_8 + \sigma_{16} + \sigma_{11} + \sigma_1$ を取得して、図3に示す処理にしたがって、以下のようにしてヤコビ和の候補値jを演算する。

【0041】

まず、図3のステップS3.1において、変数 ξ に、 $ab=21$ なので、1の原始21乗根を格納し、変数mに、 $2n / (a-1)(b-1) = 26.6 \dots$ なので、27を格納する。

【0042】

次に、図3のステップS32において、変数 r_0 に円分体 $Q(\zeta)$ のランダム整数を以下のようにして格納する。変数 r_0 を0に初期化し、 $t=0$ に対し、乱数 $r_0 = -2$ を発生し、 r_0 に $r_0 \zeta^0 = -2$ を加え、 $r_0 = -2$ とし、 $t=1$ に対し、乱数 $r_1 = 2$ を発生し、 r_0 に $r_1 \zeta^1 = 2 \zeta$ を加え、 $r_0 = -2 + 2\zeta$ とし、以下同様の操作を $t=11$ まで繰り返して、 $r_0 = -2 + 2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$ を得る。

【0043】

次に、図3のステップS33において、各整数 $i=0, 1, 2, \dots$ に対して、以下の操作を行う。 $i=0$ に対し、変数 r に $r_0 + 0$ を格納し、 $r = -2 + 2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$ を得て、そのノルム $N_{Q(\zeta)} | Q(r)$ を計算し、129571513を得てp記憶ファイル167に格納し、変数 l に $p=129571513$ のビット数29を格納し、 $l=29$ が $m=27$ 程度であることを確認し、 $p=129571513$ を既知の方法により素因数分解すると $p=129571513=43 \times 211 \times 14281$ となり $p=129571513$ は素数ではないので、 $i=0$ に対する処理を終了し、 $i=1$ に対して、同様の操作を繰り返す。本実施の形態の場合は、 $i=2$ となるまで同様の操作が続き、 $i=2$ に対し、変数 r に $r_0 + 2$ を格納し、 $r = 2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$ を得て、そのノルム $N_{Q(\zeta)} | Q(r)$ を計算し、163255597を得てp記憶ファイル167に格納し、変数 l に $p=163255597$ のビット数28を格納し、 $l=28$ が $m=27$ 程度であり、 $p=163255597$ は素数と判定されるので(素数判定には既知の手法を用いる)、ステップS33の操作は終了する。

【0044】

次に、図3のステップS34において、変数 r の値 $2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$ に、スティッケルバーガー要素 $\omega = \sigma_4 + \sigma_1 + \sigma_8 + \sigma_{16} + \sigma_{11} + \sigma_1$ を作用させ、結果をj記憶ファイル164に格納する。

【0045】

すなわち、 $j = \sigma_4(r) \sigma_{19}(r) \sigma_8(r) \sigma_{16}(r) \sigma_{11}(r) \sigma_1(r)$
 $= -11346 + 4158\zeta + 9337\zeta^2 - 10930\zeta^3 + 3060\zeta^4 + 11132\zeta^5 - 1408\zeta^6 -$

$$10000 \zeta^7 + 7506 \zeta^8 + 1237 \zeta^9 - 9894 \zeta^{10} + 16406 \zeta^{11}$$

となるので、j記憶ファイル 1 6 4 の内容は $-11346 + 4158 \zeta + 9337 \zeta^2 - 10930 \zeta^3 + 3060 \zeta^4 + 11132 \zeta^5 - 1408 \zeta^6 - 10000 \zeta^7 + 7506 \zeta^8 + 1237 \zeta^9 - 9894 \zeta^{10} + 16406 \zeta^{11}$ となる。

【0 0 4 6】

次に、位数候補値計算装置 1 3 が、図 4 に示す処理にしたがって、a記憶ファイル 1 6 1、b記憶ファイル 1 6 2、j記憶ファイル 1 6 4 からそれぞれa、b、jを取得し、以下のようにしてヤコビ群の位数の候補値を計算する。

【0 0 4 7】

まず、図 4 のステップ S 4 1 において、変数 ζ に、 $ab=21$ なので、1の原始21乗根を格納する。

【0 0 4 8】

次に、図 4 のステップ S 4 2 において、各整数 $k=1, \dots, 2ab=42$ に対して、ヤコビ和候補値 j を用いて、 $N_{Q(\zeta) | Q} (1 + (-\zeta)^k j)$ を計算し、結果を変数 h_k に格納する。すなわち、 $k=1$ に対して、 $N_{Q(\zeta) | Q} (1 + (-\zeta) j) = 18945750554224674862720917379214050968749547249577$ なので、変数 h_1 に18945750554224674862720917379214050968749547249577が格納され、 $k=2$ に対して、 $N_{Q(\zeta) | Q} (1 + (-\zeta)^2 j) = 18928969305265796978830941938772180777050417721949$ なので、変数 h_2 に18928969305265796978830941938772180777050417721949が格納される。

【0 0 4 9】

以下同様にして、変数 h_3 に18939442397757559639176586128404383479076142135761が、変数 h_4 に18935060345406437247984249590121980321244862496761が、変数 h_5 に18935622676852726684902816970612470237474541809664が、変数 h_6 に18931936903665705475581647305574444786263237069081が、変数 h_7 に18929560654771860101383318185997674116929626012889が、変数 h_8 に18939150203650250186166315242126355786799280592469が、変数 h_9 に18932675807273674693936115572103379669380378369473が、変数 h_{10} に18942309965821405414970614992239749691042375170033が、変数 h_{11} に18934229290635176830764035532046510839791719442389が、変数 h_{12} に18935834172588603026508807514961653603431968293369が、変数 h_{13}

に18938078743053945947831932134835899678969080710281が、変数 h_{14} に18930980854114698521197692341107826796840225368461が、変数 h_{15} に18925926348482126046797408190951930473609373791353が、変数 h_{16} に18936229724314338327608155999193464492913218459633が、変数 h_{17} に18935389098278487495205740285052812170943878823253が、変数 h_{18} に18931691567781542998050896522571358027374445665073が、変数 h_{19} に18932734180610926108166703609049207716180145717849が、変数 h_{20} に18938664411743724815803784593761801461579705647693が、変数 h_{21} に18933942752770105179837989473472080616474423254969が、変数 h_{22} に18919302986335777367049540268484273861903106390769が、変数 h_{23} に18936075396885270373781711765180522497408613713621が、変数 h_{24} に18925604328984592629627465194343191206594160037073が、変数 h_{25} に18929984863788418751836156261712299372083231633577が、変数 h_{26} に18929422531793648170111228339741198150094983499776が、変数 h_{27} に18933107954541528865152848804062672753166448460761が、変数 h_{28} に18935483634705487053043563594391048299333735703993が、変数 h_{29} に18925896848340062851972136696783348221127455098349が、変数 h_{30} に18932368490475205159124453933007681555744686326777が、変数 h_{31} に18922739336864448742750281538719599103232717642873が、変数 h_{32} に18930815175217344826609492375186423724694014551957が、変数 h_{33} に18929210510360406226057659372472230885175421077009が、変数 h_{34} に18926967327936730178250537884862137815188718140673が、変数 h_{35} に18934063763272126450623787600233843527396400812437が、変数 h_{36} に18939120559761876801054292506881700885415287701041が、変数 h_{37} に18928816315710623530089460607608797337081800632473が、変数 h_{38} に18929656538570982720438072809652072203857571941789が、変数 h_{39} に18933352933862176606331230531189579186007983024249が、変数 h_{40} に18932310663274994445599743180032079937147687805121が、変数 h_{41} に18926381945702726406182624557022344113037957991709が、変数 h_{42} に18931102681789095072229676262975577344314266433617が、それぞれ格納される。

【0 0 5 0】

最後に、位数候補値計算装置 1 3 は、ヤコビアン群の位数の候補値として変数

$h_1 \sim$ 変数 h_{42} の内容をHとして、H記憶ファイル165にまとめて格納する。

【0051】

次に、安全性判定装置14が、H記憶ファイル165からHを取得し、Hに含まれる位数の候補値 h_1 、 h_2 、...、 h_{42} から概素数性等の安全性条件を満たす候補値hを検索し、h記憶ファイル166に格納する。本実施の形態では、説明を簡明にするため、安全性条件は概素数性のみを検討する。既知の素数判定法を用いると、 $h_{11} = 18934229290635176830764035532046510839791719442389$ が素数と判定され、安全性判定装置14は、 $h = h_{11} = 18934229290635176830764035532046510839791719442389$ をh記憶ファイル166に格納する。

【0052】

次に、パラメータ決定装置15が、a記憶ファイル161、b記憶ファイル162、p記憶ファイル167、h記憶ファイル166からそれぞれa、b、p、hを取得し、図5に示す処理にしたがって動作する。

【0053】

まず、図5のステップS51において、変数 ζ_3 に $p=163255597$ を法とする1の原始3乗根である127994587を、変数 ζ_7 に $p=163255597$ を法とする1の原始7乗根である8342648をそれぞれ格納する。

【0054】

次に、図5のステップS52において、各整数 $l=1, 2, 3$ および各整数 $m=1, 2, 3, 4, 5, 6, 7$ に対して、以下のような処理を行う。

【0055】

まず、 $l=1$ 、 $m=1$ に対して、変数 ε に $\zeta_3 = 127994587$ を格納し、変数 η に $\zeta_7 = 8342648$ を格納し、式 $\varepsilon y^3 + \eta x^7 + 1 = 127994587 y^3 + 8342648 x^7 + 1 = 0$ で定義される代数曲線のヤコビアン群のランダムな元 $\{151707017 + 104678491x + 123646083x^2 + 18753988y + 87634493x^3 + 61274336xy + x^4, 138799785 + 145105684x + 584395x^2 + 80828873y + 34715892x^3 + 121885874xy + 59787844x^4 + x^2y, 161162224 + 117150097x + 100956100x^2 + 89380061y + 140032555x^3 + 43367019xy + y^2\}$ を生成し、これを変数Gに格納し、変数Gに格納されている点の、ヤコビアン群における $h=189342292906351768307$

64035532046510839791719442389倍を計算し、計算結果である $\{133659497 + 103424746 x + 136032897 x^2 + 131029199 y + 24618867 x^3 + 114944034 x y + x^4$ 、 $86125426 + 125891893 x + 19568269 x^2 + 27044314 y + 80420960 x^3 + 137562092 x y + x^2 y$ 、 $53604112 + 65990501 x + 51269221 x^2 + 55271502 y + 7974233 x^3 + 84922220 x y + y^2\}$ を変数Gに格納する。

【0 0 5 6】

変数Gの上記内容がヤコビアン群における単位元 $\{$ に等しくないので、次に、 $l=1$ 、 $m=2$ に対して、変数 ε に $\zeta_3 = 127994587$ を格納し、変数 η に $\zeta_7^2 = 8342648^2 \bmod 163255597 = 159772073$ を格納し、上記の処理を繰り返す。

【0 0 5 7】

本実施の形態の場合、 $l=2$ 、 $m=2$ に対して、 $\varepsilon=35261009$ 、 $\eta=159772073$ となり、ランダムに生成された点 $G = \{4568071 + 141843715 x + 68256743 x^2 + 71903501 y + 128953783 x^3 + 10781960 x y + x^4$ 、 $48272788 + 45615229 x + 150692034 x^2 + 53973350 y + 11114765 x^3 + 78550130 x y + 61331354 x^4 + x^2 y$ 、 $117552807 + 135448907 x + 64074711 x^2 + 141058974 y + 49208246 x^3 + 93940317 x y + y^2\}$ の $h=18934229290635176830764035532046510839791719442389$ 倍が単位元 $\{$ となり、パラメータ決定装置 1 5 は安全な代数曲線のパラメータとして、 $p=163255597$ 、 $\varepsilon=35261009$ 、 $\eta=159772073$ を出力する。

【0 0 5 8】

最後に、パラメータ決定装置 1 5 の出力したパラメータ $p=163255597$ 、 $\varepsilon=35261009$ 、 $\eta=159772073$ が出力装置 1 8 より出力される。

【0 0 5 9】

次に、本発明の第 2 の実施の形態について詳細に説明する。

本発明の第 2 の実施の形態は、

(a) a記憶ファイル 1 6 1、b記憶ファイル 1 6 2 から、それぞれ素数 a、b を取得し、円の ab 分体におけるスティッケルバーガー要素 ω を演算するスティッケルバーガー要素計算手順と、

(b) 前記スティッケルバーガー要素計算手順により演算されたスティッケルバーガー要素 ω を ω 記憶ファイル 1 6 3 に記憶する手順と、

(c) a記憶ファイル161、b記憶ファイル162、n記憶ファイル168、 ω 記憶ファイル163からそれぞれ素数a、素数b、暗号鍵のサイズn、ステッカー要素 ω を取得し、2つの異なる素数a、素数bに対するヤコビ和候補値jおよびヤコビ和候補値jに対応する素数pを演算するヤコビ和候補値計算手順と、

(d) 前記ヤコビ和候補値計算手順により演算された素数p、ヤコビ和候補値jをそれぞれp記憶ファイル167、およびj記憶ファイル164に記憶する手順と、

(e) a記憶ファイル161、b記憶ファイル162、j記憶ファイル164から、それぞれ素数a、素数b、ヤコビ和候補値jを取得し、素数a、素数bで指定される代数曲線のヤコビアン群の位数の複数の候補値からなる集合Hを演算する位数候補値計算手順と、

(f) 前記位数候補値計算手順により演算された集合HをH記憶ファイル165に記憶する手順と、

(g) H記憶ファイル165から集合Hを取得し、集合Hの中から概素数性等の安全性条件を満たす候補値hを検索する安全性判定手順と、

(h) 前記安全性判定手順により検索された候補値hをh記憶ファイル166に記憶する手順と、

(i) a記憶ファイル161、b記憶ファイル162、p記憶ファイル167、h記憶ファイル166からそれぞれ素数a、素数b、素数p、候補値hを取得し、素数a、素数b、素数pで指定される代数曲線でそのヤコビアン群の位数が候補値hと一致する代数曲線のパラメータを演算するパラメータ決定手順と、

を含むことを特徴とする代数曲線暗号における安全なパラメータの生成方法である。

【0060】

次に、本発明の第3の実施の形態について図面を参照して詳細に説明する。

図6は、本発明の第3の実施の形態を示すブロック図である。

図6を参照すると、本発明の第3の実施の形態は、本発明の第2の実施の形態の各手順をコンピュータ100に実行させるプログラムを記録する記録媒体130である。このプログラムは、コンピュータ100の記憶装置にロードされ実行される。

【 0 0 6 1 】

【発明の効果】

本発明の効果は、従来使用できなかった高次の複雑な代数曲線を代数曲線暗号に用いることができ、代数曲線暗号の安全性を向上することである。

【 0 0 6 2 】

その理由は、 $\alpha Y^a + \beta X^b + 1 = 0$ という形の定義方程式をもつ代数曲線のクラスから、そのヤコビアン群の位数がほぼ素数である代数曲線を効率的に探索することが可能となり、使用できる代数曲線の範囲が広がり、攻撃者の解読作業が分散増加するからである。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施の形態を示すブロック図である。

【図 2】

スティッケルバーガー要素計算装置の動作を示すフローチャートである。

【図 3】

ヤコビ和候補値計算装置の動作を示すフローチャートである。

【図 4】

位数候補値計算装置の動作を示すフローチャートである。

【図 5】

パラメータ決定装置の動作を示すフローチャートである。

【図 6】

本発明の第 3 の実施の形態を示すブロック図である。

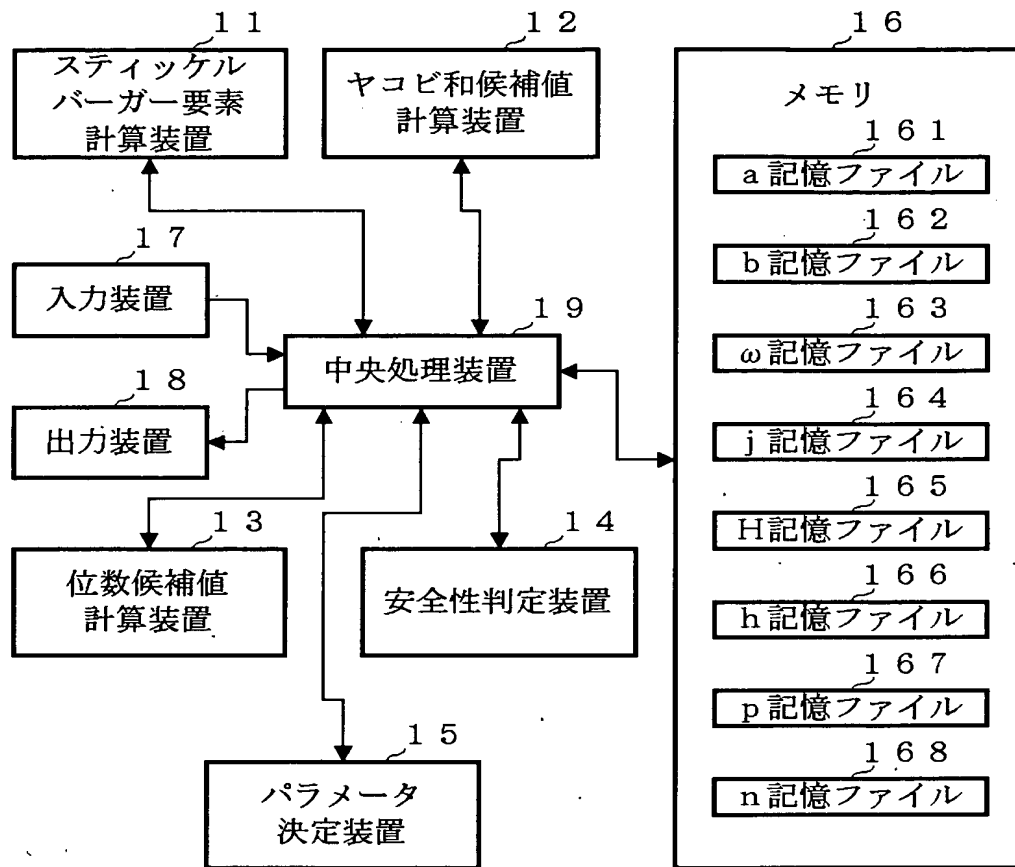
【符号の説明】

- 1 1 スティッケルバーガー要素計算装置
- 1 2 ヤコビ和候補値計算装置
- 1 3 位数候補値計算装置
- 1 4 安全性判定装置
- 1 5 パラメータ決定装置
- 1 6 メモリ

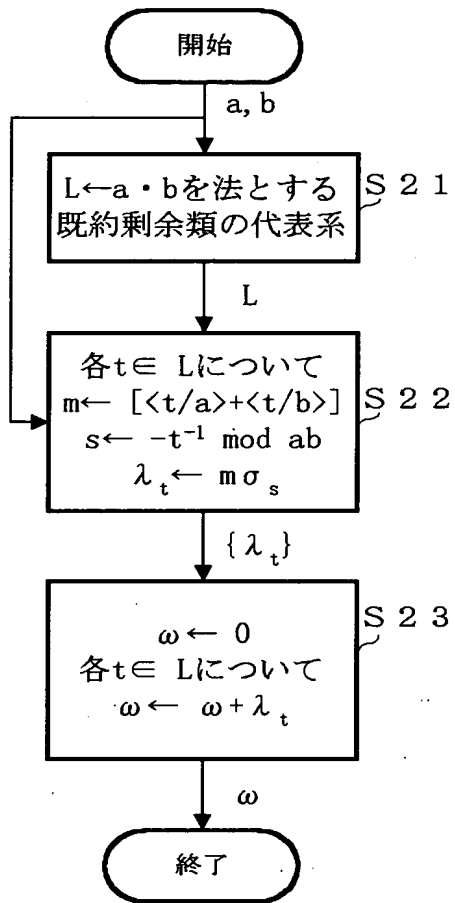
- 1 7 入力装置
- 1 8 出力装置
- 1 9 中央処理装置
- 1 0 0 コンピュータ
- 1 3 0 記録媒体
- 1 6 1 a記憶ファイル
- 1 6 2 b記憶ファイル
- 1 6 3 ω記憶ファイル
- 1 6 4 j記憶ファイル
- 1 6.5 H記憶ファイル
- 1 6 6 h記憶ファイル
- 1 6 7 p記憶ファイル
- 1 6 8 n記憶ファイル

【書類名】 図面

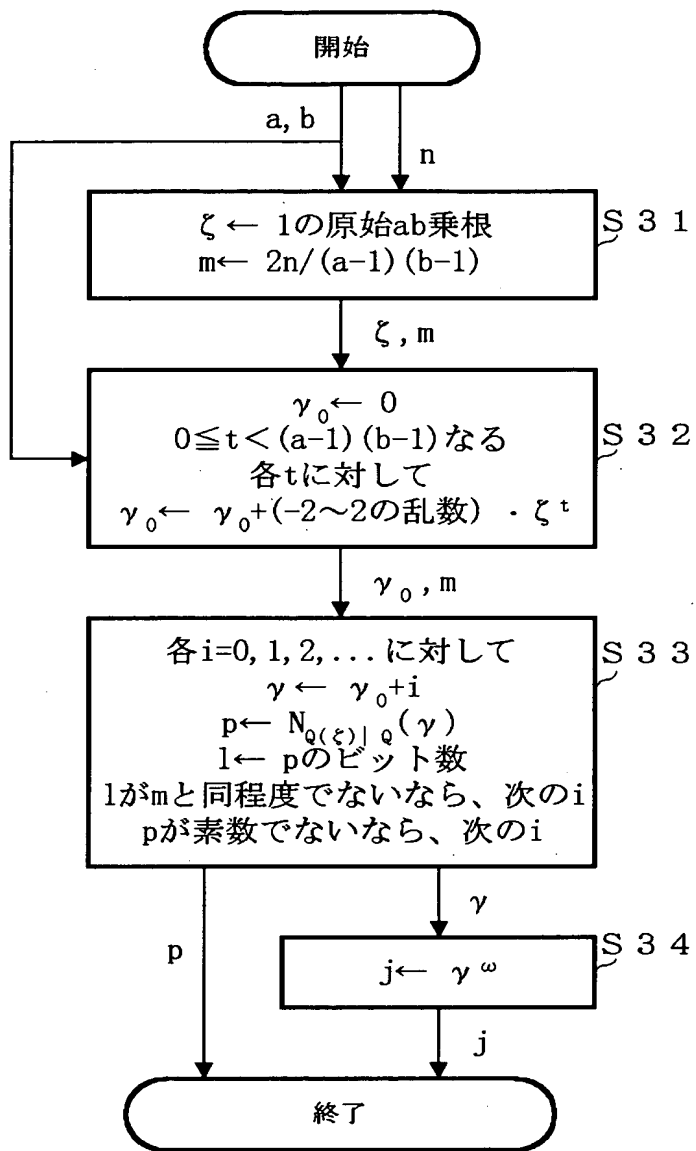
【図 1】



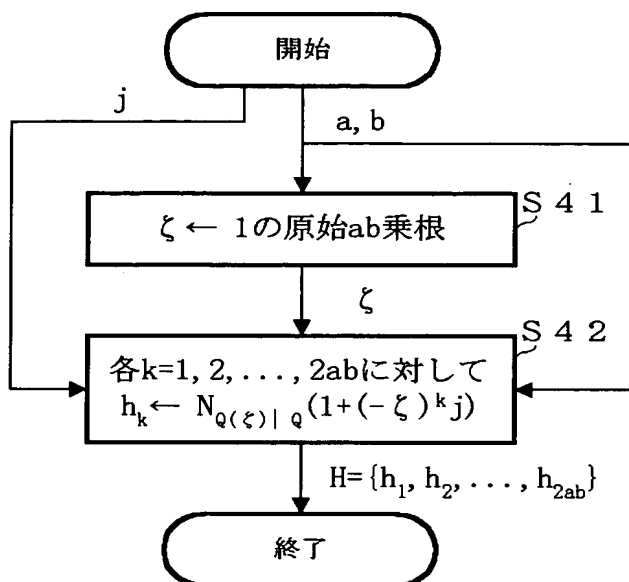
【図 2】



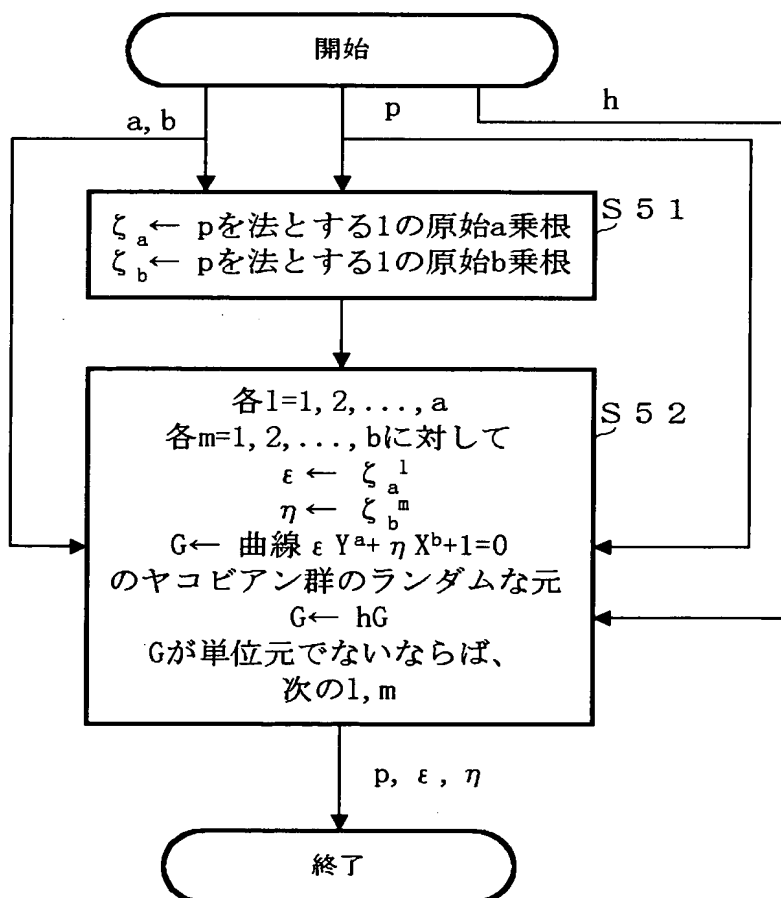
【図 3】



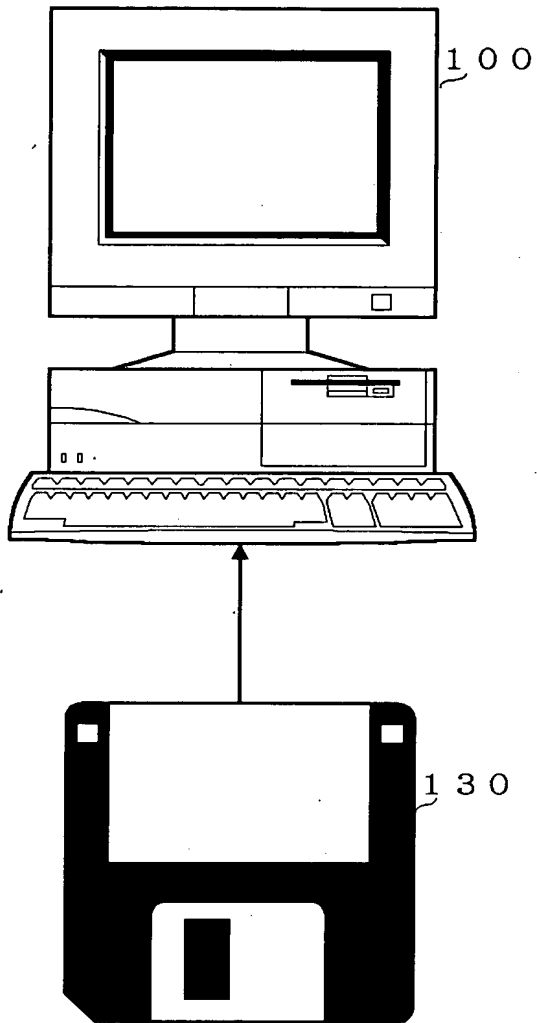
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 従来使用できなかった高次の複雑な代数曲線を代数曲線暗号に用いることを可能とし、代数曲線暗号の安全性を向上させる。

【解決手段】 スティックエルバーガー要素計算装置 1 1 が、円の ab 分体におけるスティックエルバーガー要素 ω を演算し、次に、ヤコビ和候補値計算装置 1 2 が、素数 a 、素数 b 、暗号鍵のサイズ n 、スティックエルバーガー要素 ω から、ヤコビ和候補値 j およびヤコビ和候補値 j に対応する素数 p を演算し、位数候補値計算装置 1 3 が、素数 a 、素数 b 、ヤコビ和候補値 j から、代数曲線のヤコビアン群の位数の複数の候補値からなる集合 H を演算し、安全性判定装置 1 4 が、集合 H の中から概素数性等の安全性条件を満たす候補値 h を検索し、パラメータ決定装置 1 5 が、素数 a 、素数 b 、素数 p で指定される代数曲線でそのヤコビアン群の位数が候補値 h と一致する代数曲線のパラメータを演算する。

【選択図】 図 1

認定・付加情報

特許出願の番号	平成11年 特許願 第242075号
受付番号	59900832923
書類名	特許願
担当官	第七担当上席 0096
作成日	平成11年 8月31日

<認定情報・付加情報>

【提出日】	平成11年 8月27日
-------	-------------

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 4 2 3 7]

1. 変更年月日 1 9 9 0 年 8 月 2 9 日

[変更理由] 新規登録

住 所 東京都港区芝五丁目 7 番 1 号

氏 名 日本電気株式会社